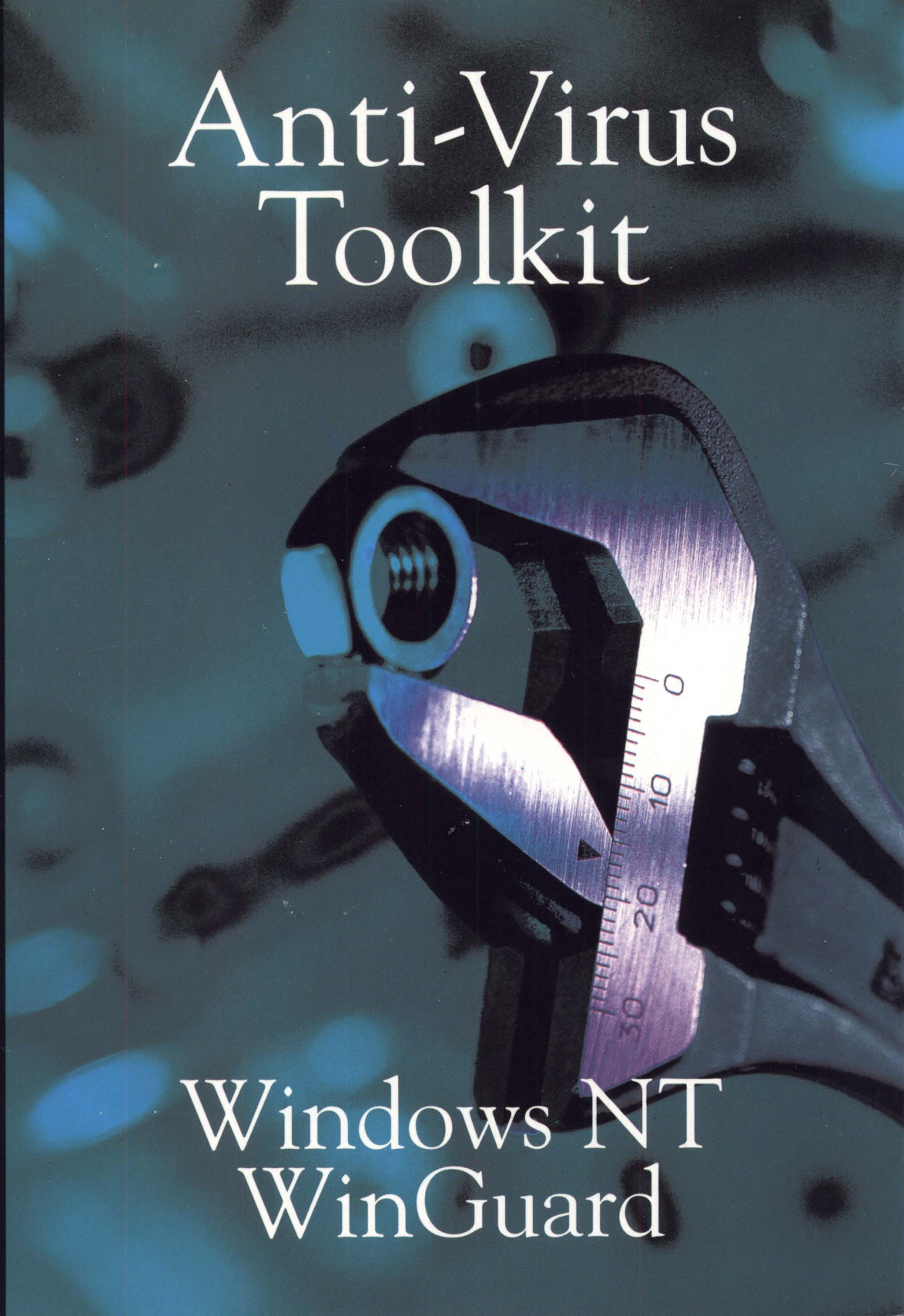
DR SOLOMON'S

# Anti-Virus Toolkit



## Windows NT WinGuard

# Dr Solomon's
# WinGuard for Windows NT


## UK Head Office: Dr Solomon's Software Ltd.

Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, UK

Tel: +44 (0)1296 318700 Fax: +44 (0)1296 318777 e-mail: support@uk.drsolomon.com

CompuServe: GO DRSOLOMON

## USA Head Office: Dr Solomon's Software, Inc.

1 New England Executive Park, Burlington, MA 01803, USA

Tel: +1 (1)617 273-7400 Fax: +1 (1)617 273-7474 e-mail: support@us.drsolomon.com

CompuServe: GO DRSOLOMON

## German Office: Dr Solomon's Software GmbH

Luisenweg 40, 20537 Hamburg, Deutschland

Tel: +49 (0)40 251954-0 Fax: +49 (0)40 251954-50 e-mail: support@de.drsolomon.com

CompuServe: GO DRSOLOMON


SS1311A-20-05

## Copyright

**Dr Solomon's Anti-Virus Toolkit for Windows and DOS** is copyright © 1996 Dr Solomon's Software Ltd. All rights reserved. Dr Solomon's Anti-Virus Toolkit for Windows and DOS is not copy-protected. This does not mean that you can make unlimited copies of it. Dr Solomon's Anti-Virus Toolkit for Windows and DOS is protected by the copyright laws which pertain to computer software. It is illegal to make copies of the program other than as may be licensed or for purposes of backup without written permission from Dr Solomon's Software Ltd. No part of the manual or other documentation accompanying Dr Solomon's Anti-Virus Toolkit for Windows and DOS may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language, in any form or by any means, without the prior written permission of Dr Solomon's Software Ltd.

### Disclaimer

Neither Dr Solomon's Software Ltd. nor anyone else who has been involved in the creation, production or delivery of Dr Solomon's Anti-Virus Toolkit for Windows and DOS or this manual makes any warranties with respect to the contents of the software or this manual and each specifically disclaims any implied warranties to the extent allowed by legislation. Dr Solomon's Software Ltd. reserves the right to revise the software and the manual and to make changes from time to time in the contents without obligation to notify any person.

### Trademarks

Dr Solomon's is a registered trademark of Dr Solomon's Software Ltd. All other product names mentioned are acknowledged to be the marks of their producing companies.

### Software release

This manual describes version 7.x of Dr Solomon's WinGuard for Windows NT.

### Manual edition

Edition 2.0
October 1996

# Contents

**Contents** ..... iii

**Preface** ..... v
Warnings and Tips ..... v
Related documentation ..... v
Windows NT documentation ..... v
Anti-Virus Toolkit for Windows NT manual ..... v
The Virus Encyclopedia ..... vi
If you need help ..... vi

**1. Introduction** ..... 1
1.1 File Scanning ..... 1
1.2 Boot and Partition Sector Scanning ..... 2
Diskettes ..... 2
Local Hard Disks ..... 2
1.3 Configuration Options ..... 3
1.4 WinGuard NT and FindVirus ..... 3

**2. Installing** ..... 5
2.1 Installing as part of Toolkit ..... 5
2.2 Installing as a separate licence ..... 5
2.3 Installing over a network ..... 5

**3. The Alert Dialog** ..... 7

**4. If a virus is found** ..... 9
4.1 What happens ..... 9
4.2 What to do ..... 9

**5. Configuring** ..... 11
5.1 Starting the Configuration Applet ..... 12
5.2 Scanner Tab ..... 13
5.3 Action Tab ..... 16
5.4 Output Tab ..... 18
5.5 FindVirus Tab ..... 21
5.6 Advanced Tab ..... 23
5.7 Statistics Tab ..... 26

This page has been left blank.

# Preface

This manual provides all the information you need to install and use WinGuard for Windows NT.

## Warnings and Tips

Throughout the text, symbols appear in the margin to draw your attention to particular points. These are as follows:

This indicates important information or tips to which you should pay particular attention.

This indicates a warning, and you should read it carefully.

## Related documentation

### Windows NT documentation

Some aspects of using WinGuard for Windows NT are standard Windows NT procedures (looking at the WinGuard NT infection reports in the Windows NT Event Log for example). Details are included in the documentation supplied with the PC and/or operating system.

### Anti-Virus Toolkit for Windows NT manual

WinGuard for Windows NT is one of the modules of the Dr Solomon's Anti- Virus Toolkit for Windows NT. See the Anti-Virus Toolkit manual for information on the other Toolkit modules.

### The Virus Encyclopedia

Included with the Dr Solomon's Anti-Virus Toolkit is a copy of the Virus Encyclopedia book. As well as giving background information about viruses, it includes details of many of the viruses that the Toolkit can detect. The Encyclopedia categorizes each virus, describes its effects and explains how it can be removed. It also lists any alternative names (aliases) by which the virus is known.

An on-line version of the Virus Encyclopedia is also included in the Toolkit. As new viruses are found, they are included in the latest Toolkit upgrade. The on-line version will always be more up-to-date than the printed copy.

## If you need help

If you have a problem while installing or running WinGuard NT, there are a number of ways in which you can obtain help.

Check the documentation carefully, including any README files on the disks as well as this manual and the help text. Make sure you have installed the software correctly. Your authorized distributor may also be able to advise you.

If you still cannot solve the problem, Dr Solomon's support staff are available to help you. This service is free of charge.

You can contact Dr Solomon's by any of the following methods:

**UK Office**

| | |
|---|---|
| By telephone: | +44 (0)1296 318700 |
| By fax: | +44 (0)1296 318734 |
| By bulletin board: | +44 (0)1296 318810 |
| By e-mail: | support@uk.drsolomon.com |

| | |
|---|---|
| By mail: | Dr Solomon's Software Ltd.<br>Alton House<br>Gatehouse Way<br>Aylesbury<br>Buckinghamshire<br>HP19 3XU<br>United Kingdom |

**US Office**

| | |
|---|---|
| By telephone: | +1 617 273 7400 |
| By fax: | +1 617 273 7474 |
| By e-mail: | support@us.drsolomon.com |
| By bulletin board: | +1 (617) 229-8804 |
| By mail: | Dr Solomon's Software, Inc.<br>1 New England Executive Park<br>Burlington, MA 01803<br>USA |

**German Office**

| | |
|---|---|
| By telephone: | +49 (0)40 251954-0 |
| By fax: | +49 (0)40 251954-50 |
| By e-mail: | support@de.drsolomon.com |
| By mail: | Dr Solomon's Software GmbH<br>Luisenweg 40<br>20537 Hamburg<br>Deutschland |

**World Wide**

| | |
|---|---|
| By CompuServe: | GO DRSOLOMON |
| World Wide Web: | http://www.drsolomon.com/ |

When you contact Dr Solomon's, it is helpful to have the following information available:

- Your name and company.
- Your serial number as printed on Installation Disk 1.
- The version of Windows NT you are using and the service pack level (if any).
- A clean (that is, virus-free) write-protected DOS system diskette.
- In the case of an application error, any error messages reported.

If possible, you should be at the PC when you call us. We may need additional information, or we may ask you to carry out some diagnostic tests.

# 1. Introduction

WinGuard for Windows NT starts when you boot up your PC. It becomes active in the background and detects viruses in files, boot sectors and partition sectors.

## 1.1 File Scanning

Only executable files, and files containing macro code, can be infected by viruses.

By default WinGuard NT scans an executable file when you try to:

- execute it,
- copy it,
- open it,
- or rename it.

If a virus is found your action is stopped and the 'Alert Dialog' is displayed to warn you.

WinGuard NT uses the following extensions to identify which files need to be scanned:

| | | |
|---|---|---|
| APP | DLL | SYS |
| BAT | DOC | XTP |
| BIN | DOT | 001 |
| CMD | EXE | 002 |
| COM | OV? | |
| DEV | QLB | |

For extra protection against infected files being stored on the disk you can select 'Scan Writes'. This prevents infected files being written to the disk from such sources as downloads from the Internet and the expansion of compressed files. Without 'Scan Writes' selected, these would not trigger a scan.

## 1.2 Boot and Partition Sector Scanning

When WinGuard NT detects a virus in a boot or partition sector it warns you with the 'Alert Dialog'.

### Diskettes

Diskettes contain a boot sector but no partition sector.

Diskette boot sectors are scanned the first time you try to access the diskette after inserting it, even if your access is only by a DIR command. If a virus is found the Alert Dialog is displayed.

WinGuard NT does not stop you accessing infected diskettes. The virus can only spread from the diskette if you try to boot the computer from it, so it is safe to copy files from the diskette (assuming the files are clean).

If you have an infected diskette in the A: drive and you reboot the PC, WinGuard NT cannot prevent infection, because the virus will be loaded from the diskette before WinGuard NT starts.

### Local Hard Disks

The boot and partition sectors of local hard disks are scanned each time the PC boots up.

Only the boot sectors of supported files systems are scanned, including NTFS, HPFS and DOS FAT systems.

If a virus is found the Alert Dialog is displayed.

## 1.3 Configuration Options

The above description of the way WinGuard NT operates applies to the way it is configured when it is installed. You can change the default configuration.

Examples of configuration options are:

- Whether all file types are scanned, or just executables.
- Whether boot and partition sectors are scanned.
- Whether files are scanned as they are written to the disk.

See "Configuring" on page 11 for full details.

## 1.4 WinGuard NT and FindVirus

WinGuard NT and FindVirus both have the same capability to detect known viruses - they share the same 'search engine'. The major difference is that WinGuard NT is constantly active and scans only one file, boot sector, or partition sector at a time. It scans boot and partition sectors when it starts, and files when they are accessed. This is opposed to FindVirus which you run as and when you think necessary, you select the drives to scan, and it finds all infections in one operation.

WinGuard NT alerts when an infected file has been found.

Other files which have not yet been accessed will not have been scanned, and they may be infected. We recommend that following a WinGuard NT alert you run a FindVirus scan; this will detect all virus infections, including the one which triggered the WinGuard NT alert.

FindVirus has the additional capability of removing viruses to leave you with a clean system. There is a section of the configuration program dedicated to setting the options FindVirus uses when started from the alert dialog - this includes whether the repair option is used.

The WinGuard NT Alert Dialog offers the option of starting FindVirus, if installed.

Starting FindVirus from the Alert Dialog has the advantage that FindVirus will search all the drives which contain an infected file, without you having to select them manually.

# 2. Installing

The method you use to install WinGuard for Windows NT will depend on whether you are installing it as:

- part of the full Dr Solomon's Anti Virus Toolkit,
- the separate licence option,
- or over a network.

## 2.1 Installing as part of Toolkit

To install WinGuard NT as part of the full Anti-Virus Toolkit, follow the installation procedure provided in the main Toolkit manual.

## 2.2 Installing as a separate licence

To install the separate licence version of WinGuard NT:

1. Insert the WinGuard for Windows NT Installation Diskette 1 into the 'A:' drive and run SETUP.EXE from it.
2. Follow the on-screen prompts.

## 2.3 Installing over a network

It is possible to install WinGuard NT over a network. Contact Dr Solomon's technical support for information.

This page has been left blank.

# 3. The Alert Dialog

This chapter describes how to use the Alert Dialog, which is displayed when WinGuard for Windows NT detects a virus.

The Virus Alert dialog has facilities for carrying out a 'quick fix' of the infection using FindVirus. If you want to perform a more thorough investigation refer to the chapter "If a virus is found" on page 9'.

You can close the Alert Dialog without taking any action. If you do this the alert will re-trigger the next time the infected sector or file is accessed.

The Alert Dialog is displayed below:

It presents a list of infection reports, which include a date and time stamp and the name of the infected file, and gives you the option of starting FindVirus or the full Toolkit (if you have these installed). The infection report list gets longer as each new infection is added. Click 'Clear' to remove all items from the list.

Use the dialog's buttons as follows:

| | |
|---|---|
| Hide | Close the dialog without clearing the infection report list. |
| Clear | Clear the infection report list.<br><br>The alert dialog remains open. Infected files listed in the Alert Dialog will re-trigger the alert the next time they are accessed. |
| Run FindVirus | Run a FindVirus scan on all the drives which contain a file featured in the infection report list.<br><br>The alert dialog is closed but the infection report list is not cleared. FindVirus will be able to remove virus infections, if the 'Repair' option is selected - see Page 21. |
| | This button is grayed out if you do not have FindVirus installed. See also "WinGuard NT and FindVirus" on page 3. |
| Start Toolkit | Start the Dr Solomon's Anti-Virus Toolkit main dialog.<br><br>The alert dialog is closed but the infection report list is not cleared. |
| | This button is grayed out if you do not have the Anti-Virus Toolkit installed. |

# 4. If a virus is found

This chapter details what happens when WinGuard for Windows NT detects a virus, and what to do about it.

## 4.1 What happens

If WinGuard for Windows NT detects a virus:

- The action you are performing is stopped.
- The Alert Dialog pops up on the screen in front of any program you are running. See "The Alert Dialog" on page 7 for an illustration of this dialog.
- Depending on the configuration options set, reports of the virus may be passed as messages and recorded in the event log. See "Output Tab" on page 18.
- Your application will probably also warn you that it cannot access the file/disk specified.
- All other system activities carry on as usual.

## 4.2 What to do

The Alert Dialog provides options for a 'quick fix', see "The Alert Dialog" on page 7. You are also advised to make a more thorough investigation as follows:

3. Note the details of the infected files from the Alert Dialog then close it. See "The Alert Dialog" on page 7.
4. Exit in the normal way and save any files you were working on.
5. Try to stop further spread of the virus; shut down any non-essential activity on the machine.

Make sure you do not shut down activity which is essential for network functioning, without proper pre-planning.

6. Refer to the chapter 'Virus Repair and Removal' in the main Toolkit manual for further instructions.

# 5. Configuring

WinGuard NT's default configuration is suitable for most situations (the configuration it has on installation). The configuration can be changed to suit your specific requirements.

Full details of the configuration options, and how to start the configuration applet, are provided in the following sections.

A brief summary of each option, with the default setting and the page number of the full explanation, is provided below.

| Option | Default setting | See Page |
|---|---|---|
| Scan executable files. | Enabled | 13 |
| Scan data files in addition to executable files. | Disabled | 14 |
| Scan boot sectors. | Enabled | 14 |
| Scan partition sectors. | Enabled | 14 |
| Scan files as they are written to the disk (in addition to scanning files as they are read). | Disabled | 14 |
| Use an extra driver containing supplementary virus information. | Disabled | 15 |
| Move infected files to a specific directory. | Disabled | 17 |
| Report infections to the Windows NT events log. | Disabled | 19 |
| Notify infections on the network. | Disabled | 19 |
| Report infections to a nominated ASCII text file. | Disabled | 20 |
| Use the 'Repair' option of FindVirus when you start it from the alert dialog. | Disabled | 21 |
| Use the 'Extra Driver' option of FindVirus when you start it from the alert dialog. | Disabled | 22 |
| Use the 'Report File' option of FindVirus, to the nominated file, when you start it from the alert dialog. | Disabled | 22 |

| Option | Default setting | See Page |
|---|---|---|
| Set the maximum number of concurrent scans (uses Windows NT multi-threading). Default figure is 'per processor'. | 4 | 24 |
| Avoid unnecessary repeat scanning of files. | 149 | 24 |
| Avoid unnecessary repeat scanning of files when accessed over the network. | Disabled | 25 |
| Clear the list of scan exempt files. | | 25 |
| Display statistics (this is not strictly a configuration option). | | 26 |

## 5.1 Starting the Configuration Applet

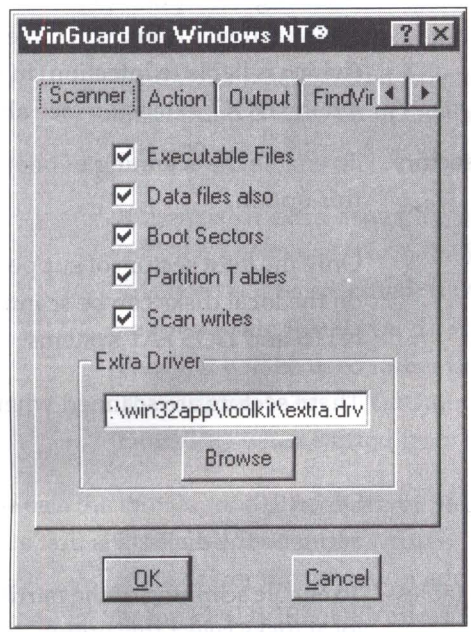
To configure WinGuard NT start the configuration applet located in the Control Panel.

A multiple tab dialog box is displayed. Click on a tab to bring it to the front. You can scroll through the tabs by using the '►' and '◄' buttons at the top.

Full details on using each of the tabs are provided in the following sections.

## 5.2 Scanner Tab

The Scanner Tab sets what areas are scanned and when files are scanned. It also sets whether an extra driver is used.




The configuration options are.

Executable Files — To enable the scanning of executable files select this option.

Deselecting 'Executable Files' also deselects 'Data files also'.

You would deselect 'Executable Files' if you only wanted to scan boot and/or partition sectors.

See page 1 for a list of file extensions that WinGuard uses to distinguish executable files.

Data files also

To scan data files as well as executable files select this option.

Selecting this option also selects 'Executable Files'.

Selecting this option provides extra security, perhaps if you think you have macro code (which is liable to infection) in documents with a non '.DOC' extension (see also page 1).

Boot sectors

To enable the scanning of boot sectors select this option.

Only the boot sectors of supported file systems on the local disks can be scanned, including NTFS and DOS FAT systems.

These sectors are scanned when the PC boots up.

Diskette boot sectors are also scanned, when access to the diskette is first attempted.

Partition tables

To enable scanning of the partition tables of the local disks select this option.

Partition tables are scanned when the PC boots up.

Scan writes

To enable the scanning of files as they are written to the disk select this option.

See page 1 for more information.

Extra Driver

To specify an extra driver file enter its name into the box. Select the file's name from the 'Browse' interface (click on the 'Browse' button), or type it directly into the box. You cannot specify an extra driver which is located on a remote machine.

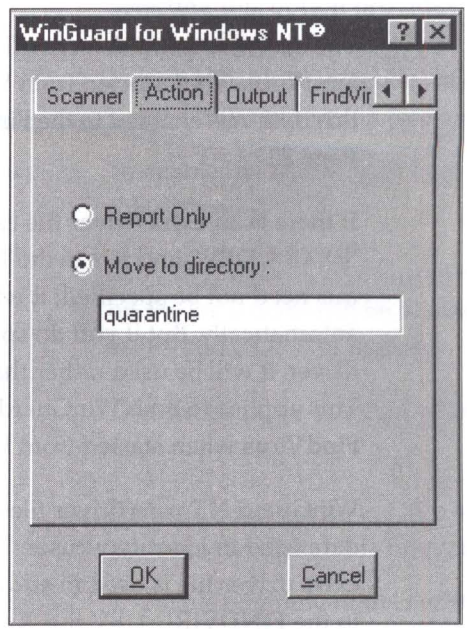
The specified extra driver will also be used by FindVirus when started from WinGuard NT, if this option is enabled in the FindVirus tab - see Page 22.

If there is an extra driver file called 'EXTRA.DRV', and it is in the Toolkit directory, this need not be specified; it will be used automatically. But if you do specify an extra driver, it will be used rather than EXTRA.DRV. This applies to both WinGuard NT and FindVirus when started from WinGuard NT.

WinGuard NT uses driver files to contain the data used to identify viruses. The data in the extra driver file is used in addition to the data in the FINDVIRU.DRV file. Extra drivers are occasionally produced as an interim measure between monthly updates to cover specific virus outbreaks.

## 5.3 Action Tab

Use the Action Tab to set what actions WinGuard NT takes on detecting a virus.




The configuration options are:

Report only — To perform all the alert actions, without moving the infected file to a directory, select this option.

The 'Move to directory' will be de-selected.

Move to directory

To store all infected files in one directory select 'Move to directory' and enter the directory's name in the box.

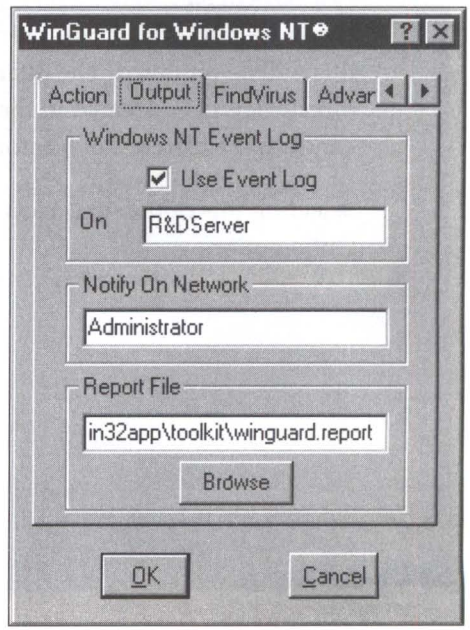
If you enter a new directory name and/or path it will be created the first time an infected file needs to be moved.

If you specify a drive letter for the directory this will be removed. The quarantine path/directory will be created in the drive that contains the infected file, before it is moved.

Selecting this option deselects the 'Report Only' option.

## 5.4 Output Tab

The Output Tab sets the reports which WinGuard NT makes on finding a virus. WinGuard NT makes the reports in addition to displaying the Alert Dialog.



The configuration options are:

**Windows NT Event Log**

To copy infection reports to the Windows NT event log select 'Use Event Log'.

If you want to divert the reports to another computer on the network enter the computer's name in the 'On' box.

The event reports will appear as copies of the text seen in the Alert Dialog.

To see the event reports use the Windows NT Event Viewer, and look at the 'Application Log'. They have the category 'WinGuard NT'. Refer to your Windows NT documentation for details.

**Notify on Network**

To send a report of infections to another computer, or user, on the network, enter the name of the computer or user into the box.

Winguard NT uses the Windows NT messaging service for this facility.

This option has no affect on the 'Report File' and 'Windows NT Event Log' options.

Report File

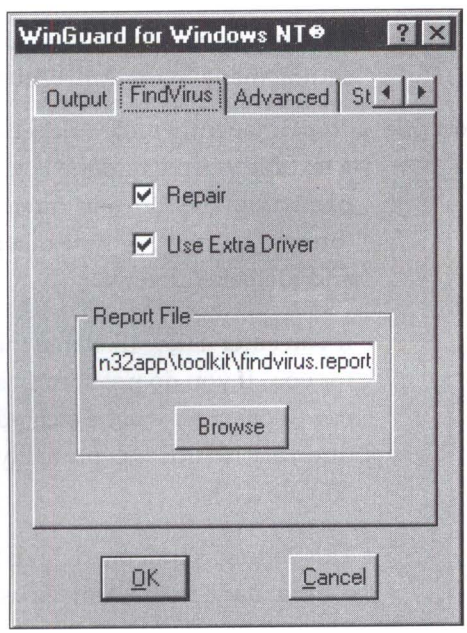
To keep a permanent record of infection reports enter a text file's name into the box. Select the file's name from the 'Browse' interface (click on the 'Browse' button), or type in a path (optional) and filename directly.

If you enter a new filename this will be created for you. If you do not specify a path for the new filename it will be created in the toolkit directory (which will probably be the default 'TOOLKIT').

Each infection report line that the virus alert dialog displays (see "The Alert Dialog" on page 7) is also copied into the specified file. Report lines are added to the existing text.

## 5.5 FindVirus Tab

You are given the option of starting FindVirus after an Alert Dialog is displayed (if FindVirus is installed). FindVirus Tab allows you to set the options that FindVirus uses. See the main toolkit documentation for details of FindVirus.




The configuration options are:

Repair — To repair viruses when FindVirus is run, select this option.

Use Extra Driver

For FindVirus to start with an extra driver enabled, select this option.

Extra drivers are occasionally produced as an interim measure between scheduled driver updates to cover specific virus outbreaks. The extra driver's name is specified in the Scanner Tab (see Page 15).

This setting is independent of the FindVirus setting made in the Anti-Virus Toolkit.

Report File

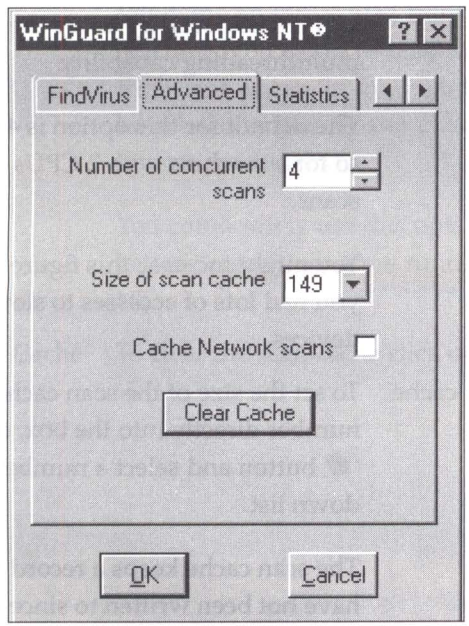
To permanently record infection reports enter a text file's name into the box. Select the file's name from the 'Browse' interface (click on the 'Browse' button), or type in a path (optional) and filename directly.

If you enter a new filename this will be created for you. If you do not specify a path for the new filename it will be created in the Toolkit directory (which will probably be the default 'TOOLKIT').

This setting is independent of the FindVirus setting made in the Anti-Virus toolkit.

## 5.6 Advanced Tab

Use the Advanced Tab to fine tune the technical configuration options of WinGuard NT. The default configuration of this tab will be adequate for most users. If you feel you do need to make changes, proceed with caution and make sure you are aware of the consequences.



The configuration options are

Number of concurrent scans

To set the maximum number of files which can be scanned simultaneously type a new number into the box, or use the '▼' button to decrement the number, or the '▲' button to increment the number.

Concurrent scans optimize processor usage, and are achieved by using the WinGuard NT multithreading capability.

The default for this option is 4 scans per CPU, so for a machine with 2 CPUs this would be 8 scans.

You might increase this figure if, for example, you had lots of accesses to slow storage devices.

Size of scan cache

To set the size of the scan cache type a new number directly into the box, or click on the '▼' button and select a number from the drop down list.

The scan cache keeps a record of files which have not been written to since they were last scanned. As files can only be changed by a write accesses, these files are not scanned again, this prevents unnecessary delays.

The advantage of increasing the scan cache size is that files are less likely to be scanned unnecessarily, but the disadvantage is that more memory is used to contain the cache.

Cache Network scans

To record files read from a remote machine in the scan cache select this option.

This option must be used with EXTREME CAUTION. Writes to a file which is made on a remote machine will not remove the file's entry from the scan cache (unlike writes made on the local machine). This means that following an initial read from a remote machine, you could re-read the file without triggering a scan, in the meantime the file may have been written to and infected on the remote machine.

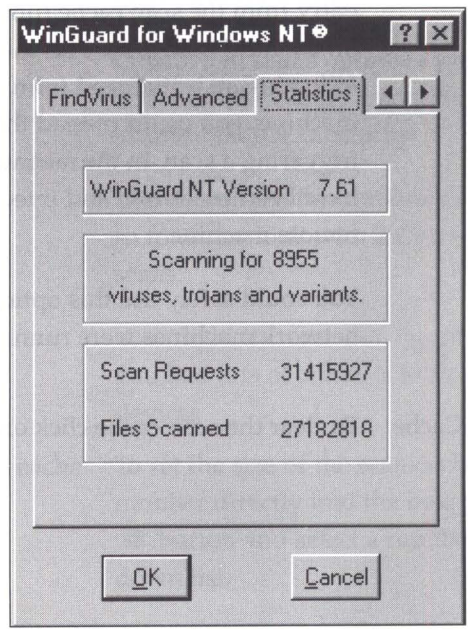
You could safely use this option if all the network machines were running WinGuard NT.

Clear Cache

To clear the scan cache click on this button.

## 5.7 Statistics Tab

The Statistics Tab reports statistics on scanning activity. It is not strictly a configuration tab.




The report items are as follows:

Version number — This is the current version number of the Anti-Virus Toolkit.

New versions are released as the driver file is updated with new virus information, and as the product is developed.

You can be automatically supplied with new versions if you subscribe to Dr Solomon's monthly or quarterly updating service. See the addresses in the preface.

| | |
|---|---|
| Scanning for NNNN viruses, trojans and variants | This is the number of known viruses trojans and variants whose characteristic 'fingerprint' WinGuard NT is looking for.<br><br>This item changes with each release as new viruses are added to the driver file, to be included in the detection capability of the product. |
| Scan requests | This is the number of file accesses which have been made since WinGuard NT was started.<br><br>This will be greater than the actual number of files scanned, as accesses to non-executable files, and accesses to files recorded in the scan cache, do not result in a scan. |
| Files scanned | Since WinGuard NT was started, this is the actual number of scans which WinGuard NT has performed. |

This page has been left blank.

# Index

A
Action Configuration Tab 16
Advanced Configuration Tab 23
Alert Dialog 7, 9, 18

B
Boot sectors 2
Boot sectors - configuration item 14

C
Cache Network scans - configuration item 25
Clear Cache button 25
Compressed files 1

D
Data files also - configuration item 14

E
Executable Files - configuration item 13
Extra Driver - configuration item 15

F
Files scanned statistic 27
FindVirus Configuration Tab 21

I
Installing 5
Internet 1

M
Move to directory - configuration item 17

N
Notify on Network - configuration item 19
Number of concurrent scans - configuration option 24
Number of viruses - searching for statistic 27

O
Output Configuration Tab 18

P
Partition tables - configuration item 14

R
README files vi
Repair - configuration option 21
Report File - configuration item 20, 22
Report only - configuration item 16

S
Scan requests statistic 27
Scan writes - configuration item 14
Scanner Configuration Tab 13
Size of scan cache - configuration item 24
Statistics display 26
Support addresses vi

T
technical support vi

U
Use Extra Driver - configuration item 22

V
Version number statistic 26
Virus Encyclopaedia vi
Virus Encyclopedia vi

W
Windows NT Event Log - configuration item 19